Computer CSI

Other

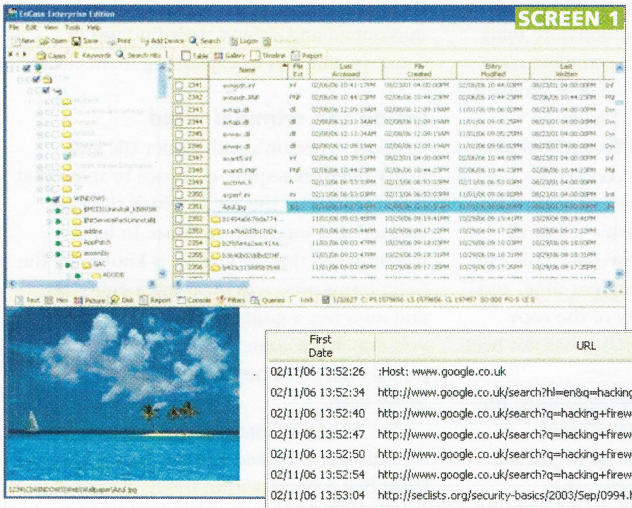
Computer CSI

PCs are increasingly becoming a vital source of clues for solving today's high-tech crimes, as computer forensics expert Ian Kennedy explains

Think of a TV programme with a crime scene and there are usually some common components – a body, a bloodstained weapon and a couple of glasses covered in fingerprints for a murder, perhaps. But what of the computer sitting in the corner? Could this contain evidence of contact between the victim and their killer? Increasingly, you'll see the computer bagged as evidence too, in shows like *CSI* or *Without a Trace*.

The relatively new field of computer forensics is, like other forensic sciences, becoming a popular area for study at the moment, and not just because of the TV. With virtually everyone using a computer, demand for forensic analysts and the availability of post-graduate courses for those who want to learn about computer forensics are both on the increase.

The use of forensic evidence from computers and other digital devices has become a common feature in investigating many crimes. No longer are computers simply seen as tools to commit a crime such as fraud; they can now bear witness to events leading up to other crimes, such as research and planning, or email exchanges between the suspect and victim.



Left: Encase software can produce a complete copy of a hard disk

Below: A suspect's internet history can provide proof of a guilty mind

SCREEN 2

First Date	URL	
02/11/06 13:52:26	:Host: www.google.co.uk	AdamW
02/11/06 13:52:34	http://www.google.co.uk/search?hl=en&q=hacking+firewalls&meta=	AdamW
02/11/06 13:52:40	http://www.google.co.uk/search?q=hacking+firewalls&hl=en&lr=&start=10&sa=N	AdamW
02/11/06 13:52:47	http://www.google.co.uk/search?q=hacking+firewalls&hl=en&lr=&start=20&sa=N	AdamW
02/11/06 13:52:50	http://www.google.co.uk/search?q=hacking+firewalls&hl=en&lr=&start=30&sa=N	AdamW
02/11/06 13:52:54	http://www.google.co.uk/search?q=hacking+firewalls&hl=en&lr=&start=40&sa=N	AdamW
02/11/06 13:53:04	http://seclists.org/security-basics/2003/Sep/0994.html	AdamW
02/11/06 13:54:08	http://insecure.org/nmap/index.html	AdamW
02/11/06 13:54:13	http://insecure.org/nmap/download.html	AdamW
02/11/06 13:54:39	http://download.insecure.org/nmap/dist/nmap-4.11-setup.exe	AdamW
02/11/06 13:54:53	http://insecure.org/nmap/install/inst-windows.html	AdamW

The digital post-mortem

In a criminal investigation, procedure and documentation are the two most important factors that determine how an examination is conducted. The forensic analyst works methodically through a process that can be split into four broad stages – acquisition, identification, evaluation and presentation.

Acquisition is concerned with the forensically sound capture and preservation of digital and physical evidence, which is paramount for the investigation. The computer and its hard drives are crime scenes in their own right and must be secured and preserved, so once the computer has been seized, every sector of the hard disk has to be captured to produce a forensically sound copy.

You can't just rush in and connect the disk from a seized computer to a forensic computer to examine it – Windows may write data to the drive as soon as it detects it. The problems don't stop there either; as soon as you access files or folders on the disk their associated Last Access dates and times will be updated, potentially destroying valuable information. Even if this sort of mistake is avoided, there is a good chance virus checking software on the forensic computer will almost certainly try to check the disk, quarantining any suspect files it finds. To sidestep these difficulties, forensic examiners use a piece of equipment called a hardware write-blocker, which is designed to stop all write

Convicted by complacency

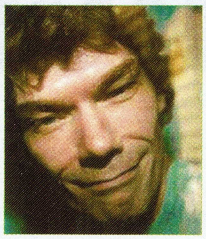
One of the most prolific serial killers in the world, Dr Harold Shipman, was outwitted by a combination of ignorance and arrogance. During his interview, Shipman told police: "I'm sorry I'm smiling, you have no concept of general practice." Of all the evidence stacked against him, it was the compelling forensic computer evidence unearthed by detective sergeant John Ashley that was to prove the most damning to his case.

In an attempt to cover his tracks, Shipman had backdated and fabricated medical records stored on his practice computer, to support a cause of death that he would provide. One of his victims, Kathleen Grundy, had died on 24 June 1998. Examination of the practice computer revealed a database record dated by Shipman as 23 June 1997, indicating that she was 'depressed although always happy'. Unknown to him, his computer was making an audit of all his entries, recording every entry with a date and a time stamp automatically. This same entry had an audited entry date of 25 June 1998 – the day after Mrs Grundy had died.

Tripped up by time zones

"The biggest military computer hack of all time." That's how the US Government described the allegations against Glasgow-born Gary McKinnon, who was accused of bypassing the security of what should be among the most sophisticated computer systems on the planet. These belonged to the US Department of Defense, Nasa and other high-profile organisations.

For all his care and planning in moving around the networks, McKinnon slipped up as a result of a simple mistake. "I got caught because I was using a graphical remote-control tool, and I forgot what time zone I was in," McKinnon said. "Somebody was in the office when I was moving the mouse around."



McKinnon hacked into US Government systems

commands reaching the hard disk, effectively rendering it a read-only device.

There are several forensic software tools available that can produce a complete copy of the disk in a series of files. Some products, such as Encase (see screen 1) from Guidance Software (**www.guidancesoftware.com**), and the FTK Imager from Accessdata (**www.accessdata.com**) generate and embed a Message Digest 5 (MD5) hash – a sort of digital fingerprint – into these files. This can be regenerated at any subsequent time, and used to validate the integrity of the copy being examined, showing that it has not been tampered with.

Assuming acquisition goes smoothly, the next stage of forensic examination is identification. This is largely about placing facts into context. For example, at a physical level, a note is made of how many hard disks are present in the computer and which was configured as the boot disk. At the logical level, the partitioning arrangement on the disks and the file systems on them can perhaps reveal the level of knowledge possessed by the computer's owner. Identifying the file system is also important in interpreting the layout of the disk and the behaviour of files as they are created, moved and deleted.

The evaluation stage of the process is concerned with locating and evaluating evidence. Here, the strategy used by the forensic analyst will depend on a number of factors, including the alleged crime, the number of exhibits and whether the suspect is in custody, on bail or not yet arrested.

For a forensic computer analyst undertaking work for a criminal prosecution, the presentation stage of the work is ultimately destined for an audience of lay people in a court of law. Much of the data found on a computer is stored in a raw format, and interpreting the information will usually be beyond the technical knowledge and experience of the jury and other people in court. A key task for the analyst, then, is to interpret the data and present it without opinion, using only facts and probabilities to add weight to any significant evidence. A forensic scientist must be prepared to be questioned and defend their findings in court, in addition to explaining them clearly.

Inside the criminal mind

To prove a person's guilt under UK law, many offences require evidence to show that they committed the act of which they are accused and intended to do so. In legal terminology, this distinction is known by the Latin terms *actus reus* meaning a guilty act and *mens rea*, a guilty mind. These are terms you may have come across if you've done jury service. Computer forensics can help prove both.

For example, imagine that a business has recently been hacked and the police have identified a suspect from the IP addresses in the firewall logs, tracing the IP address back, via the ISP, to a particular person. Now, suppose confidential company files are found during an examination of the suspect's computer. This provides evidence of *actus reus*. By investigating the suspect's internet history on the computer, a forensic analyst discovers a number of Google searches that were carried out just prior to the offence, using the search phrase 'hacking firewalls' (see screen 2).

The analysis also shows that the user went through a further four pages of results from Google, before visiting the site **http://insecure.org** and downloading the file nmap-4.11.setup.exe. This website and tool are network security related, so the activity is indicative of their thinking process, or *mens rea*.

Future forensics

Everything we've looked at so far has taken place on a static snapshot of the computer. Conventional practice advocates that if a computer was powered on at the time of seizure, it should be powered down to prevent any changes to the data. But what evidence can you potentially lose by doing this? And is there another way to analyse the system?

Encrypted file systems, for example, are becoming easier to implement, and harder to crack. The Bitlocker technology built into Windows Vista (see *PCW*, December 2006 and **www.pcw.co.uk/2166361**) is Microsoft's response to the growing problem of lost or stolen laptops containing sensitive data. It provides a high level of security, even preventing data being read when a disk is transferred to another computer. And, of course, it may not be possible to persuade the computer's owner to hand over the recovery key, even if they can be found. So, what better way to bypass this technology than to simply analyse the computer while it is still up and running – an emerging area called 'live forensics'. Another benefit is the potential capture and study of volatile data in memory – for example, a suspect might have a command-line history full of incriminating commands and IP addresses.

Of course, this is not a pure forensic approach; even with minimal contact, small changes will be made to the computer's memory. Crucially, though, the impact of such analysis can be predicted and minimised, usually by using specific tools that are made up of static rather than dynamically compiled code, minimising any potential changes to the system being observed.

As computers develop, with ever more security built in, forensic analysis will adapt too, whether by live analysis or in other ways, to make sure that vital evidence can be preserved and examined. Much of what you see on TV – such as the perfect enhancement of reflections on a pair of spectacles in a digital photo – may be fanciful, but computer forensics are an increasingly important and effective tool in the fight against crime. **PCW**

Forensic principles

In the UK, the Association of Chief Police Officers (ACPO) has laid down four principles to be followed by everyone involved in computer forensic examinations:

- The data held on an exhibit must not be changed.
- Any person accessing the exhibit must be competent to do so, and explain the relevance and implications of their actions.
- A record of all processes applied to an exhibit should be kept and must be repeatable to an independent third party.
- The person in charge of the investigation has responsibility for ensuring that the law and these principles are adhered to.